UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/530,293	04/04/2005	Mats Naslund	3995-42	4649

23117 7590 02/06/2009

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
SCHWARTZ, DARREN B	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
02/06/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/530,293	NASLUND ET AL.	
	Examiner	Art Unit	
	DARREN SCHWARTZ	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 December 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *44-78* is/are pending in the application.

4a) Of the above claim(s) *63-78* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *44-62* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 April 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *04-04-05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Applicant amends claims 63, 64 and 77. Claims 44-78 are presented for examination.

Election/Restrictions

Claims 63-78 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected species, there being no allowable generic or linking claim. Election was made **without** traverse in the reply filed on 24 December 2008.

Applicant's election without traverse of Species I with claims 44-62 in the reply filed on 24 December 2008 is acknowledged.

Claim 44 is generic to the disclosed patentably distinct species. The species are independent or distinct because as disclosed the different species have mutually exclusive characteristics for each identified species. In addition, these species are not obvious variants of each other based on the current record.

Upon the allowance of a generic claim, applicant will be entitled to consideration of claims to additional species which depend from or otherwise require all the limitations of an allowable generic claim as provided by 37 CFR 1.141.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

1. Claim 52 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitations "at least of the environment" and "and the network interface." There is insufficient antecedent basis for said limitations in the claim.

Any claim not specifically addressed above is being rejected as incorporating the deficiencies of a claim upon which it depends.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 44-59 and 61 are rejected under 35 U.S.C. 102(b) as being anticipated by "Wireless Identity Module," 12 July 2001, Wireless Application Protocol, WAP-260-WIM-20010712-a, hereinafter referred to as WIM.

Re claim 44: WIM teaches a tamper-resistant security device (page 12: "*Smart card a device with an embedded microprocessor chip. A smart card is used for storing data and performing typically security related (cryptographic) operations. In WAP context, a smart card may be the GSM Subscriber Identity Module (SIM) or a card used in a secondary card reader of a WAP phone.*") having memory for storing user credentials, including at least a security key, an Authentication and Key Agreement (AKA) module for performing an AKA process with said security key (page 8: "*The WAP Identity Module (WIM) is used in performing WTLS and application level security functions, and especially, to store and process information needed for user identification and authentication. The functionality presented here is based on the requirement that sensitive*

data, especially keys, can be stored in the WIM, and all operations where these keys are involved can be performed in the WIM."), and external communication circuitry (page 8: "*An example of a WIM implementation is a smart card. In the phone, it can be the Subscriber Identity Module (SIM) card or an external smart card.*"), wherein said tamper-resistant security device further comprises: an application for cooperation with said AKA module (page 8: "*PKI functionality (including WTLS client authentication with private keys, and WMLScript digital signatures) can be implemented in pure software in normal PDAs or phones, using password protection, encryption etc. However, such implementations cannot be considered as WIM implementations, and are out of scope of this specification. At the same time, service interfaces defined in this specification may be useful for designing internal software interfaces for these implementations;*" page 63: "The WIM application may have to reside on the card with other applications, eg, GSM. It is selected using an Application Identifier (AID) which is a combination of a Registered Application Provider Identifier (RID) and a Proprietary Application Identifier Extension (PIX) [ISO7816-5]."); and

an interface for interfacing said AKA module and said cooperating application (page 8: "This specification concentrates on defining an interface between the part of a WAP client device…;" page 15: "Use of generic cryptographic features with standard interfaces like ISO7816 and PKCS#15 can make it interesting to use the WIM also for non-WAP applications, like SSL, TLS, S/MIME etc;" page 63: "The WIM application may have to reside on the card with other applications, eg, GSM. It is selected using an Application Identifier (AID) which is a combination of a Registered Application Provider Identifier (RID) and a Proprietary Application Identifier Extension (PIX) [ISO7816-5].").

Re claim 45: WIM teaches cooperating application performs enhanced security processing of at least one parameter associated with said AKA process (page 15: "The information structure is based on [PKCS15] which enables a flexible information format on a cryptographic token. It uses on object model that makes it possible to access keys, certificates, authentication objects and proprietary data objects in a simple device (with simple read/write, and access control features);" page 18: "Digital signing may be used for authentication or non-repudiation purposes (eg, sign a document or confirm a transaction). For non-repudiation, a separate key is usually used, and the user is requested to enter authentication information (PIN) for every signature made. Note that in order to support non-repudiation, the signature key must never leave a tamper-resistant device. For signing some data, the ME calculates a hash of the data, formats it according to the requirements of the application and sends the formatted hash to the WIM. The WIM calculates the digital signature using the private key, and returns the digital signature.").

Re claim 46: WIM teaches enhanced security processing includes at least one of: pre-processing of at least one AKA input parameter; and post-processing of at least one AKA output parameter (page 26: section 7.2.4.6; page 31: "Establishing pre-master secret").

Re claim 47: WIM teaches enhanced security processing includes encapsulation of said at least one AKA parameter (page 21: section 7.2.2.1; page 43: section 9.4.6).

Re claim 48: WIM teaches cooperating application is receiving at least one AKA parameter from said AKA process to generate a further AKA parameter that has higher security than said received AKA parameter (page 8: "This specification does not define exact requirements for tamper-resistance. Businesses can enforce certain requirements and policies using PKI based mechanisms. Applications should only accept certificates signed by Certification Authorities that

are known to fulfill the requirements and policies. PKI functionality (including WTLS client authentication with private keys, and WMLScript digital signatures) can be implemented in pure software in normal PDAs or phones, using password protection, encryption etc. However, such implementations cannot be considered as WIM implementations, and are out of scope of this specification. At the same time, service interfaces defined in this specification may be useful for designing internal software interfaces for these implementations.").

Re claim 49: WIM teaches enhanced security processing includes evaluation of a predetermined number of consecutive AKA input parameters for verifying that said AKA input parameters can be used securely (page 18: "Signature verification by WIM may be used in cases where an application needs verification capability (e.g. certificate or end entity signature verification) but the verification algorithm is not present in the ME, or the verification algorithm implementation is more efficient in the WIM.").

Re claim 50: WIM teaches enhanced security processing further includes combination of a predetermined number of consecutive AKA output parameters generated in response to a number of corresponding unique AKA input parameters (see various APDU commands: pages 74-78).

Re claim 51: WIM teaches means for performing security policy processing based on information representative of security conditions in relation to said tamper-resistant security device (page 8: "A basic requirement for WIM implementation is that it is tamper-resistant;" page 8: "This specification does not define exact requirements for tamper-resistance. Businesses can enforce certain requirements and policies using PKI based mechanisms. Applications should only accept certificates signed by Certification Authorities that are known to fulfill the requirements and policies.").

Re claim 52: WIM teaches the security conditions reflect at least one of the environment in which said security device is operated and the network interface over which a request for AKA processing originates (page 8: "The Wireless Application Protocol (WAP) is a result of continuous work to define an industry-wide specification for developing applications that operate over wireless communication networks.").

Re claim 53: WIM teaches security policy processing includes at least one of a security policy decision process and a security policy enforcement process (page 8: "This specification does not define exact requirements for tamper-resistance. Businesses can enforce certain requirements and policies using PKI based mechanisms. Applications should only accept certificates signed by Certification Authorities that are known to fulfill the requirements and policies.").

Re claim 54: WIM teaches means for performing security policy processing comprises means for selectively disabling direct access to said AKA module (page 95: "In a typical case, the PIN-G is used to protect all files (which need to be protected) and keys except non-repudiation keys. If the PIN-G is not disabled, the ME must send the PIN-G after the WIM application is selected, in order to be able to use keys and perform other operations that require the PIN-G. More precisely, the ME SHOULD do the following when the secure functions are required the first time.").

Re claim 55: WIM teaches tamper-resistant security device comprises means for detecting whether said tamper-resistant security device is operated in its normal environment or in an environment considered insecure (page 49: "For the WAP-WTLS application there are two predefined SEs with their associated number."), and said means for performing security policy

processing comprises means for disabling direct access to said AKA module when operated in said insecure environment (page 95: "In a typical case, the PIN-G is used to protect all files (which need to be protected) and keys except non-repudiation keys. If the PIN-G is not disabled, the ME must send the PIN-G after the WIM application is selected, in order to be able to use keys and perform other operations that require the PIN-G. More precisely, the ME SHOULD do the following when the secure functions are required the first time.").

Re claim 56: WIM teaches said cooperating application includes a security enhancing application, and said security device further comprises means for transferring a request for AKA processing directly to said AKA module if said security device is operated in an environment considered secure, and means for transferring said request to said security enhancing application if said security device is operated in an environment considered insecure (page 74, section 11.3.6.4: "PERFORM SECURITY OPERATIONS").

Re claim 57: WIM teaches cooperating application is performing at least part of the computations in connection with end-to-end key agreement between users (page 26, section 7.2.4.5: "WIM-KeyAgreement").

Re claim 58: WIM teaches cooperating application is masking key information generated by said AKA module (page 17: "The WIM is used to protect permanent, typically certified, private keys. The WIM stores these keys and performs operations using these keys." Page 18: "Application level security operations that use the WIM include signing and unwrapping a key").

Re claim 59: WIM teaches cooperating application is a software application installed in an application environment of said tamper-resistant security device (page 63: "The WIM application may have to reside on the card with other applications, eg, GSM. It is selected using an Application

Identifier (AID) which is a combination of a Registered Application Provider Identifier (RID) and a Proprietary Application Identifier Extension (PIX) [ISO7816-5].").

Re claim 61: WIM teaches cooperating application is a privacy enhancing application, which participates in managing a user pseudonym (page 12: "A tamper-resistant device which is used in performing WTLS and application level security functions, and especially, to store and process information needed for user identification and authentication.").

3. Claim 44 is rejected under 35 U.S.C. 102(b) as being anticipated by Hopkins (U.S. Pat 5757918 A), hereinafter referred to as Hopkins.

Re claim 44: Hopkins teaches a tamper-resistant security device (Fig 1, elt 10 comprising elements: 12, 22, 26 & 20; "…smart card 12…," "…less secure facility 22…," "…secure communications from the card issuer site over a network 26…," "…secure facility 20;" particularly elt 12) having memory for storing user credentials (Fig 2, elt 12; col 4, lines 57-66), including at least a security key (col 4, line 67), an Authentication and Key Agreement (AKA) module for performing an AKA process with said security key (col 6, lines 27-30 and lines 58-59), and external communication circuitry (Fig 1, elts 25 & 26; col 4, lines 36-53), wherein said tamper-resistant security device further comprises:

an application for cooperation with said AKA module (col 4, lines 33-35); and

an interface for interfacing said AKA module and said cooperating application (Fig 1, elts 25 & 26 col 4, lines 36-53).

4. Claims 44, 51, 54 rejected under 35 U.S.C. 102(b) as being anticipated by Vatanen et al (WO 00/48416), hereinafter referred to as Vatanen.

Re claim 44: Vatanen teaches a tamper-resistant security device having memory for storing user credentials, including at least a security key (page 3, lines 4-5; page 4, lines 3-7), an Authentication and Key Agreement (AKA) module for performing an AKA process with said security key (page 3, lines 4-5; page 18, lines 5-7 and 17-21), and external communication circuitry (Fig 6, elts: 67 & 68; page 16, line 23), wherein said tamper-resistant security device further comprises:

an application for cooperation with said AKA module (page 1, lines 5-11); and

an interface for interfacing said AKA module and said cooperating application (page 1, lines 5-11; page 2, lines 17-20; page 3, lines 12-15).

Re claim 51: Vatanen teaches means for performing security policy processing based on information representative of security conditions in relation to said tamper-resistant security device (page 16, lines 26-34).

Re claim 54: Vatanen teaches means for performing security policy processing comprises means for selectively disabling direct access to said AKA module (page 4, lines 10-14; page 12, lines 28-32).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claim 60 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wireless Identity Module," 12 July 2001, Wireless Application Protocol, WAP-260-WIM-20010712-a, hereinafter referred to as WIM, in view of Vatanen et al (WO 00/48416), hereinafter referred to as Vatanen.

Re claim 60: WIM teaches all the limitations of claim 59 as previously discussed.

However, Vatanen teaches said application is securely downloaded into said tamper-resistant security device from a trusted party (page 4, line 34 – page 5, line 3).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of WIM with the teachings of Vatanen, for the purpose of installing authenticate applications on a portable device, as is known in the art.

Claim 62 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wireless Identity Module," 12 July 2001, Wireless Application Protocol, WAP-260-WIM-20010712-a, hereinafter referred to as WIM, in view of Miyoshi (U.S. Pat Pub 2003/0074570 A1), hereinafter referred to as Miyoshi.

Re claim 62: WIM teaches all the limitations of claim 61 as previously discussed.

However, Vatanen teaches said privacy enhancing application is requesting an AKA response from said AKA module based on an old user pseudonym and for generating a new user pseudonym based on the received AKA response (Fig 5: elements "RETURN TEMPORARY INTERFACE ID" and "DISTRIBUTE NEW REAL INTERFACE ID").

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of WIM with the teachings of Vatanen, for the purpose of updating access information on portable devices, as is known in the art.

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the text of the passage taught by the prior art or disclosed by the examiner.

In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARREN SCHWARTZ whose telephone number is (571)270-3850. The examiner can normally be reached on 8am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. S./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435